

# Hardware Manual for the Model CG814WG Wireless Cable Modem Gateway

## **NETGEAR**

**NETGEAR**, Inc.  
4500 Great America Parkway  
Santa Clara, CA 95054 USA  
Phone 1-888-NETGEAR

SM-CG814WGNA-Comcast-0  
October 2003

© 2003 by NETGEAR, Inc. All rights reserved.

## **Trademarks**

NETGEAR is a trademark of Netgear, Inc.

Microsoft, Windows, and Windows are registered trademarks of Microsoft Corporation.

Other brand and product names are registered trademarks or trademarks of their respective holders.

## **Statement of Conditions**

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice.

NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

## **Federal Communications Commission (FCC) Compliance Notice: Radio Frequency Notice**

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

## **EN 55 022 Declaration of Conformance**

This is to certify that the CG814WG Wireless Cable Modem Gateway is shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022 Class B (CISPR 22).

## **Certificate of the Manufacturer/Importer**

It is hereby certified that the CG814WG Wireless Cable Modem Gateway has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example,

test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

### **Voluntary Control Council for Interference (VCCI) Statement**

This equipment is in the second category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in such residential areas.

When used near a radio or TV receiver, it may become the cause of radio interference.

Read instructions for correct handling.

### **Technical Support**

Thank you for choosing Comcast as your Internet Service Provider and Netgear product(s). Please register online and take advantage of the technical support resources such as Netgear online knowledge base. Technical support is available twenty-four hours a day, seven days a week; please call your local Comcast office.



# Contents

<b>About This Manual</b> .....	<b>ix</b>
Audience .....	ix
Typographical Conventions .....	ix
Special Message Formats .....	x
<b>Chapter 1</b>	
<b>Hardware Overview</b> .....	<b>1-1</b>
About the CG814WG .....	1-1
Built-in Cable Modem .....	1-1
A Powerful, True Firewall .....	1-1
802.11g Standards-based Wireless Networking .....	1-2
Configurable Auto Uplink™ Ethernet Connection .....	1-2
USB Port .....	1-3
Protocol Support .....	1-3
Easy Installation and Management .....	1-3
What's in the Box? .....	1-5
The Gateway's Front Panel .....	1-5
The Gateway's Rear Panel .....	1-7
<b>Chapter 2</b>	
<b>Preparing Your Network</b> .....	<b>2-1</b>
Preparing Your Computers for TCP/IP Networking .....	2-1
Configuring Windows 98 SE and Me for TCP/IP Networking .....	2-2
Install or Verify Windows Networking Components .....	2-2
Enabling DHCP .....	2-4
Selecting Windows' Internet Access Method .....	2-6
Verifying TCP/IP Properties .....	2-6
Configuring Windows 2000 or XP for TCP/IP Networking .....	2-7
Install or Verify Windows Networking Components .....	2-7
DHCP Configuration of TCP/IP in Windows XP or 2000 .....	2-8
DHCP Configuration of TCP/IP in Windows XP .....	2-8

DHCP Configuration of TCP/IP in Windows 2000 .....	2-11
Verifying TCP/IP Properties for Windows XP and 2000 .....	2-14
Verifying the Readiness of Your Internet Account .....	2-15
Are Login Protocols Used? .....	2-15
What Is Your Configuration Information? .....	2-15
Obtaining ISP Configuration Information from Your Computer .....	2-16
Restarting the Network .....	2-17
<b>Appendix A</b>	
<b>Troubleshooting</b> .....	<b>A-1</b>
Basic Functions .....	A-1
Power LED Not On .....	A-2
Test LED Stays On .....	A-2
Local Link LEDs Not On .....	A-2
Cable Link LED Not On .....	A-3
Troubleshooting the ISP Connection .....	A-3
Troubleshooting a TCP/IP Network Using a Ping Utility .....	A-3
Testing the LAN Path to Your Gateway .....	A-3
Testing the Path from Your PC to a Remote Device .....	A-4
Erasing the Current/Restoring the Factory Configuration .....	A-5
<b>Appendix B</b>	
<b>Glossary</b> .....	<b>B-1</b>
<b>Appendix C</b>	
<b>Configuring Wireless Security in Windows XP</b> .....	<b>C-1</b>
What You Will Need Before You Begin .....	C-1
Observe Location and Range Guidelines .....	C-1
Two Basic Operating Modes .....	C-2
CG814WG Default Wireless Configuration Settings .....	C-3
Basic Installation Instructions .....	C-4
For Windows XP Users Installing a CG814WG .....	C-4
Wireless Connection Indicators .....	C-8
Interpreting the LED on the CG814WG .....	C-8
Interpreting System Tray Icon Colors .....	C-9
Basic Troubleshooting Tips .....	C-10
<b>Appendix D</b>	
<b>Networks, Routing, and Firewall Basics</b> .....	<b>D-1</b>
Related Publications .....	D-1

Basic Router Concepts .....	D-1
What is a Router? .....	D-2
Routing Information Protocol .....	D-2
IP Addresses and the Internet .....	D-2
Netmask .....	D-4
Subnet Addressing .....	D-5
Single IP Address Operation Using NAT .....	D-7
MAC Addresses and Address Resolution Protocol .....	D-8
Related Documents .....	D-9
Domain Name Server .....	D-9
IP Configuration by DHCP .....	D-10
Internet Security and Firewalls .....	D-10
What is a Firewall? .....	D-10
Stateful Packet Inspection .....	D-11
Ethernet Cabling .....	D-11
Uplink Switches and Crossover Cables .....	D-11
Cable Quality .....	D-12





# About This Manual

Thank you for purchasing the NETGEAR™ CG814WG Wireless Cable Modem Gateway.

This manual describes the features of the gateway and provides installation and configuration instructions.

## Audience

---

This reference manual assumes that the reader has basic to intermediate computer and Internet skills. However, basic computer network, Internet, firewall, and PC networking technologies tutorial information is provided in the Appendices.

## Typographical Conventions

---

This guide uses the following typographical conventions:

<i>italics</i>	Media titles, UNIX files, commands, URLs, and directory names.
<b>bold times roman</b>	User input
<code>courier font</code>	Screen text, user-typed command-line entries.
[Enter]	Named keys in text are shown enclosed in square brackets. The notation [Enter] is used for the Enter key and the Return key.
[Ctrl]+C	Two or more keys that must be pressed simultaneously are shown in text linked with a plus (+) sign.
SMALL CAPS	File and directory names.

## Special Message Formats

---

This guide uses the following formats to highlight special messages:



**Note:** This format is used to highlight information of importance or special interest.



**Warning:** This format is used to highlight information about the possibility of injury or equipment damage.



**Danger:** This format is used to alert you that there is the potential for incurring an electrical shock if you mishandle the equipment.

# Chapter 1

## Hardware Overview

This chapter describes the features of the NETGEAR CG814WG Wireless Cable Modem Gateway.

### About the CG814WG

---

The NETGEAR CG814WG Wireless Cable Modem Gateway connects directly to the wide area network (WAN) using its built-in cable modem. It has multiple options to connect to your local area network (LAN), including a 4-port 10/100 Mbps Ethernet switch, a USB port and an 802.11g wireless Access Point.

The CG814WG Gateway is a complete security solution that protects your network from attacks and intrusions. Unlike simple Internet sharing routers that rely on Network Address Translation (NAT) for security, the CG814WG uses Stateful Packet Inspection for attack protection and intrusion detection. The CG814WG provides highly reliable Internet access for up to 253 users.

The CG814WG offers the following features.

### Built-in Cable Modem

The CG814WG Gateway connects directly the WAN using an integrated cable modem. The modem is DOCSIS 2.0 compliant and compatible with DOCSIS 1.0 and DOCSIS 1.1, guaranteeing that it will work with your local cable service provider.

### A Powerful, True Firewall

Unlike simple Internet sharing NAT routers, the CG814WG is a true firewall, using stateful packet inspection to defend against hacker attacks. Its firewall features include:

- Automatically detects and thwarts attacks such as Ping of Death, SYN Flood, LAND Attack and IP Spoofing.
- Configurable Port Forwarding, Port Blocking, Port Triggering and DMZ provide enough flexibility for most applications.
- Blocks access from your LAN to Internet locations or services that you specify as off-limits.
- Logs security incidents  
The CG814WG will log security events such as blocked incoming traffic, port scans, attacks, and administrator logins. You can configure the gateway to email the log to you whenever a significant event occurs.

## 802.11g Standards-based Wireless Networking

The CG814WG Gateway includes an 802.11g-compliant wireless access point, providing continuous, high-speed 54 Mbps access between your wireless and Ethernet devices. The access point provides:

- 802.11g Standards-based wireless networking at up to 54Mbps, interoperable with 802.1b networks
- 64-bit and 128-bit WEP encryption security
- WEP keys can be generated manually or by passphrase
- Wireless access can be restricted by MAC address.

## Configurable Auto Uplink™ Ethernet Connection

With its internal 4-port 10/100 switch, the CG814WG can connect to either a 10 Mbps standard Ethernet network or a 100 Mbps Fast Ethernet network. Both the local LAN and the Internet WAN interfaces are autosensing and capable of full-duplex or half-duplex operation.

The gateway incorporates Auto Uplink™ technology. Each LOCAL Ethernet port will automatically sense whether the Ethernet cable plugged into the port should have a ‘normal’ connection such as to a PC or an ‘uplink’ connection such as to a switch or hub. That port will then configure itself to the correct configuration. This feature also eliminates the need to worry about crossover cables, as Auto Uplink will accommodate either type of cable to make the right connection.

## USB Port

A USB connection for your computer eliminates the need for installing an Ethernet card.

## Protocol Support

The CG814WG supports the Transmission Control Protocol/Internet Protocol (TCP/IP).

[Appendix D, "Networks, Routing, and Firewall Basics"](#) provides further information on TCP/IP.

- **IP Address Sharing by NAT**  
The CG814WG allows several networked PCs to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your Internet service provider (ISP). This technique, known as Network Address Translation (NAT), allows the use of an inexpensive single-user ISP account.
- **Automatic Configuration of Attached PCs by DHCP**  
The CG814WG dynamically assigns network configuration information, including IP, gateway, and domain name server (DNS) addresses, to attached PCs on the LAN using the Dynamic Host Configuration Protocol (DHCP). This feature greatly simplifies configuration of PCs on your local network.
- **DNS Relay**  
When DHCP is enabled and no DNS addresses are specified, the gateway provides its own address as a DNS server to the attached PCs. The gateway obtains actual DNS addresses from the ISP during connection setup and forwards DNS requests from the LAN.

## Easy Installation and Management

You can install, configure, and operate the CG814WG within minutes after connecting it to the network. The following features simplify installation and management tasks:

- **Browser-based management**  
Browser-based configuration allows you to easily configure your gateway from almost any type of personal computer, such as Windows, Macintosh, or Linux. A user-friendly Setup Wizard is provided and online help documentation is built into the browser-based Web Management Interface.
- **Diagnostic functions**  
The gateway incorporates built-in diagnostic functions such as Ping, DNS lookup, and remote reboot. These functions allow you to test Internet connectivity and reboot the gateway. You can use these diagnostic functions directly from the CG814WG when you are connect on the LAN or when you are connected over the Internet via the remote management function.

- Visual monitoring  
The gateway's front panel LEDs provide an easy way to monitor its status and activity.

## What's in the Box?

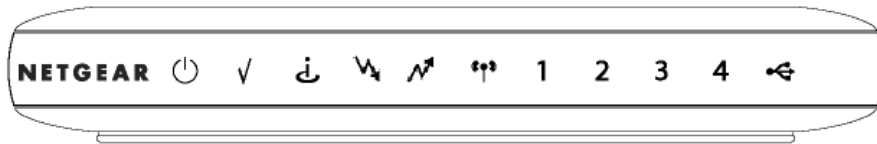
The product package should contain the following items:

- CG814WG Wireless Cable Modem Gateway
- AC power adapter
- Category 5 (CAT5) Ethernet cable
- USB cable
- *Resource CD*, including:
  - This manual
  - Application Notes, Tools, and other helpful information

If any of the parts are incorrect, missing, or damaged, contact your NETGEAR dealer. Keep the carton, including the original packing materials, in case you need to return the product for repair.

## The Gateway's Front Panel


The front panel of the CG814WG (Figure 1-1) contains status LEDs.










**Figure 1-1: CG814WG Front Panel**

You can use some of the LEDs to verify connections. [Table 1-1](#) lists and describes each LED on the front panel of the CG814WG Gateway. These LEDs are green when lit.

**Table 1-1. LED Descriptions**

Label	Activity	Description
Power 	On Off	Power is supplied to the gateway. Power is not supplied to the gateway.

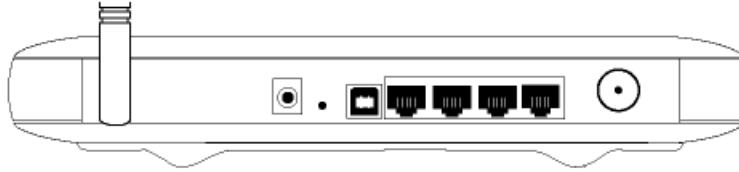
**Table 1-1. LED Descriptions**

<p>Test</p> 	<p>On Off</p>	<p>A system failure has occurred. Reboot the gateway. Normal operation.</p>
<p>Cable Link</p> 	<p>On (Green) Off</p>	<p>Configuration of the cable interface by your cable service provider is complete. Configuration of the cable interface is still in progress.</p>
<p>Cable Downstream Traffic</p> 	<p>On Off</p>	<p>Data is being received from the network to the gateway on the cable interface. The cable interface is idle.</p>
<p>Cable Upstream Traffic</p> 	<p>On Off</p>	<p>Data is being transmitted from the gateway to the network on the cable interface. The cable interface is idle.</p>
<p>Wireless</p> 	<p>On Blink</p>	<p>Indicates that the wireless Access Point is operating normally. Data is being transmitted or received on the wireless interface.</p>
<p>Local (Local Area Network)</p> 	<p>On (Green) Blink (Green) On (Yellow) Blink (Yellow) Off</p>	<p>The Local port has detected link with a 100 Mbps device. Data is being transmitted or received at 100 Mbps. The Local port has detected link with a 10 Mbps device. Data is being transmitted or received at 10 Mbps. No link is detected on this port.</p>
<p>USB</p> 	<p>On (Green) Blink (Green) Off</p>	<p>The Local port has detected link with a USB device. Data is being transmitted or received through USB. No link is detected on the USB port.</p>



## The Gateway's Rear Panel

The rear panel of the CG814WG (Figure 1-2) contains the connections identified below.



**Figure 1-2: CG814WG Rear Panel**

Viewed from left to right, the rear panel contains the following elements:

- 802.11g Wireless antenna
- AC power adapter input
- Factory Default Reset push button
- USB port for connecting the gateway to a local computer
- Four Ethernet RJ-45 ports for connecting the gateway to local computers
- Coaxial F-type connector for connecting the gateway to your cable service provider



# Chapter 2

## Preparing Your Network

This appendix describes how to prepare your network to connect to the Internet through the CG814WG Wireless Cable Modem Gateway and how to verify the readiness of broadband Internet service from an Internet service provider (ISP).



**Note:** If an ISP technician configured your computer during the installation of a broadband modem, or if you configured it using instructions provided by your ISP, you may need to copy the current configuration information for use in the configuration of your gateway. Write down this information before reconfiguring your computers. Refer to [page 2-16](#) for further information.

### Preparing Your Computers for TCP/IP Networking

---

Computers access the Internet using a protocol called TCP/IP (Transmission Control Protocol/Internet Protocol). Each computer on your network must have TCP/IP installed and selected as its networking protocol. If a Network Interface Card (NIC) is already installed in your PC, then TCP/IP is probably already installed as well.

Most operating systems include the software components you need for networking with TCP/IP:

- All Windows® 98 SE or later includes the software components for establishing a TCP/IP network.

In your IP network, each PC and the gateway must be assigned a unique IP addresses. Each PC must also have certain other IP configuration information such as a subnet mask (netmask), a domain name server (DNS) address, and a default gateway address. In most cases, you should install TCP/IP so that the PC obtains its specific network configuration information automatically from a DHCP server during bootup. For a detailed explanation of the meaning and purpose of these configuration items, refer to [Appendix D, “Networks, Routing, and Firewall Basics.”](#)

The CG814WG Gateway is shipped preconfigured as a DHCP server. The gateway assigns the following TCP/IP configuration information automatically when the PCs are rebooted:

- PC or workstation IP addresses—192.168.0.2 through 192.168.0.254

- Subnet mask—255.255.255.0
- Gateway address (the gateway)—192.168.0.1

These addresses are part of the IETF-designated private address range for use in private networks.

## **Configuring Windows 98 SE and Me for TCP/IP Networking**

---

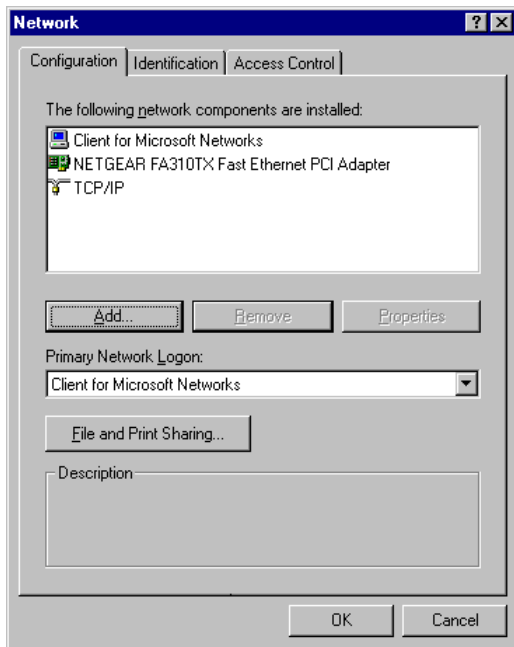
As part of the PC preparation process, you need to manually install and configure TCP/IP on each networked PC. Before starting, locate your Windows CD; you may need to insert it during the TCP/IP installation process.

### **Install or Verify Windows Networking Components**

To install or verify the necessary components for IP networking:

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Network icon.

The Network window opens, which displays a list of installed components:



You must have an Ethernet adapter, the TCP/IP protocol, and Client for Microsoft Networks.



**Note:** It is not necessary to remove any other network components shown in the Network window in order to install the adapter, TCP/IP, or Client for Microsoft Networks.

If you need to install a new adapter, follow these steps:

- a. Click the Add button.
- b. Select Adapter, and then click Add.
- c. Select the manufacturer and model of your Ethernet adapter, and then click OK.

If you need TCP/IP:

- a. Click the Add button.
- b. Select Protocol, and then click Add.
- c. Select Microsoft.
- d. Select TCP/IP, and then click OK.

If you need Client for Microsoft Networks:

- a. Click the Add button.
  - b. Select Client, and then click Add.
  - c. Select Microsoft.
  - d. Select Client for Microsoft Networks, and then click OK.
3. Restart your PC for the changes to take effect.

## Enabling DHCP

After the TCP/IP protocol components are installed, each PC must be assigned specific information about itself and resources that are available on its network. The simplest way to configure this information is to allow the PC to obtain the information from a DHCP server in the network.

You will find there are many similarities in the procedures for different Windows systems when using DHCP to configure TCP/IP.

The following steps will walk you through the configuration process for each of these versions of Windows.

**1**

Locate your **Network Neighborhood** icon.

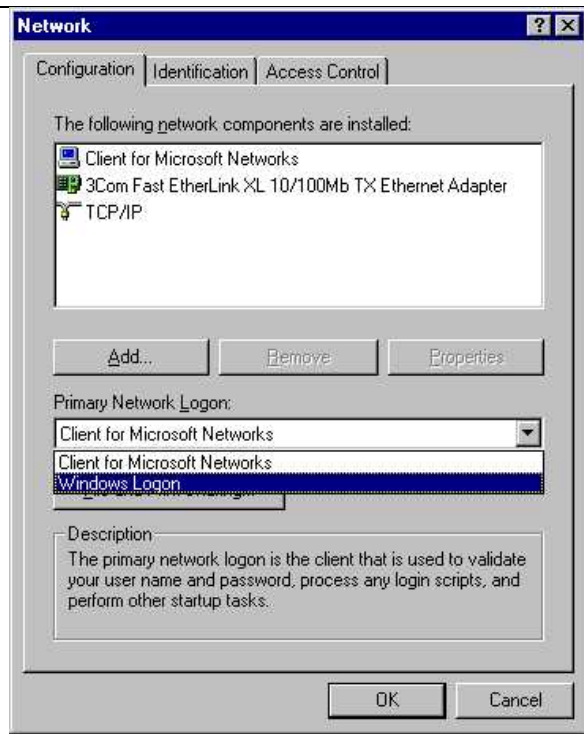
- If the Network Neighborhood icon is on the Windows desktop, position your mouse pointer over it and right-click your mouse button.
- If the icon is not on the desktop,
  - Click **Start** on the task bar located at the bottom left of the window.
  - Choose **Settings**, and then **Control Panel**.
  - Locate the **Network Neighborhood** icon and click on it. This will open the Network panel as shown below.

## 2

Verify the following settings as shown:

- Client for Microsoft Network exists
- Ethernet adapter is present
- TCP/IP is present
- **Primary Network Logon** is set to Windows logon

Click on the **Properties** button. The following TCP/IP Properties window will display.

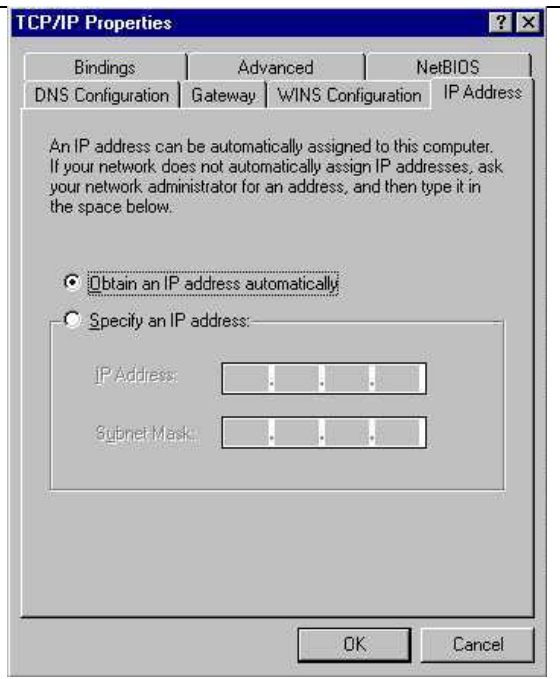


3

By default, the **IP Address** tab is open on this window. Verify the following:

- **Obtain an IP address automatically** is selected. If not selected, click in the radio button to the left of it to select it. This setting is required to enable the DHCP server to automatically assign an IP address.
- Click **OK** to continue.
- Restart the PC.

Repeat these steps for each PC with this version of Windows on your network.



## Selecting Windows' Internet Access Method

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Internet Options icon.
3. Select "I want to set up my Internet connection manually" or "I want to connect through a Local Area Network" and click Next.
4. Select "I want to connect through a Local Area Network" and click Next.
5. Uncheck all boxes in the LAN Internet Configuration screen and click Next.
6. Proceed to the end of the Wizard.

## Verifying TCP/IP Properties

After your PC is configured and has rebooted, you can check the TCP/IP configuration using the utility *wiipcfg.exe*:

1. On the Windows taskbar, click the Start button, and then click Run.



2. Type `winiipcfg`, and then click OK.

The IP Configuration window opens, which lists (among other things), your IP address, subnet mask, and default gateway.

3. From the drop-down box, select your Ethernet adapter.

The window is updated to show your settings, which should match the values below if you are using the default TCP/IP settings that NETGEAR recommends for connecting through a router or gateway:

- The IP address is between 192.168.0.2 and 192.168.0.254
- The subnet mask is 255.255.255.0
- The default gateway is 192.168.0.1

## **Configuring Windows 2000 or XP for TCP/IP Networking**

---

As part of the PC preparation process, you may need to install and configure TCP/IP on each networked PC. Before starting, locate your Windows CD; you may need to insert it during the TCP/IP installation process.

### **Install or Verify Windows Networking Components**

To install or verify the necessary components for IP networking:

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Network and Dialup Connections icon.
3. If an Ethernet adapter is present in your PC, you should see an entry for Local Area Connection. Double-click that entry.
4. Select Properties.
5. Verify that 'Client for Microsoft Networks' and 'Internet Protocol (TCP/IP)' are present. If not, select Install and add them.
6. Select 'Internet Protocol (TCP/IP)', click Properties, and verify that "Obtain an IP address automatically is selected.
7. Click OK and close all Network and Dialup Connections windows.
8. Then, restart your PC.

## DHCP Configuration of TCP/IP in Windows XP or 2000

You will find there are many similarities in the procedures for different Windows systems when using DHCP to configure TCP/IP.

The following steps will walk you through the configuration process for each of these versions of Windows.

### DHCP Configuration of TCP/IP in Windows XP

1

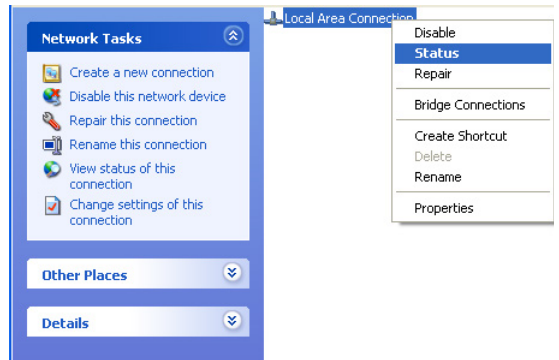
Locate your **Network Neighborhood** icon.

- Select **Control Panel** from the Windows XP new Start Menu.
- Select the **Network Connections** icon on the Control Panel. This will take you to the next step.

2

Now the Network Connection window displays. The Connections List that shows all the network connections set up on the PC, located to the right of the window.

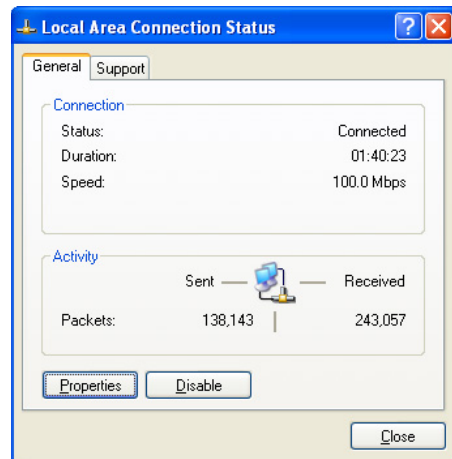
- Right-click on the **Connection with the wireless icon** and choose **Status**.



3

Now you should be at the Local Area Network Connection Status window. This box displays the connection status, duration, speed, and activity statistics.

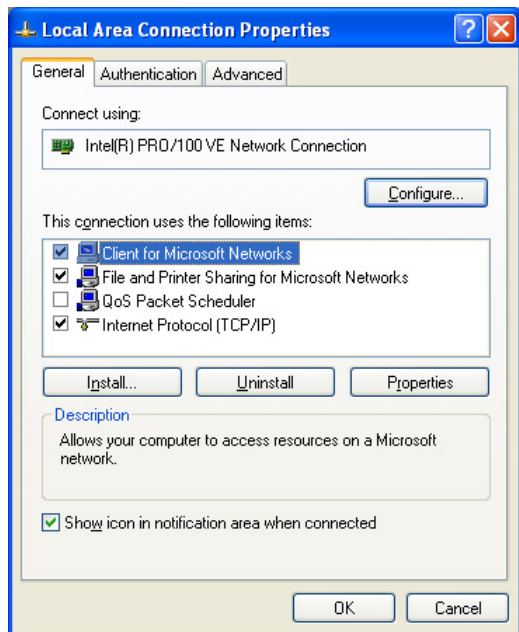
- Administrator logon access rights are needed to use this window.
- Click the **Properties** button to view details about the connection.



4

The TCP/IP details are presented on the Support tab page.

- Select **Internet Protocol**, and click **Properties** to view the configuration information.



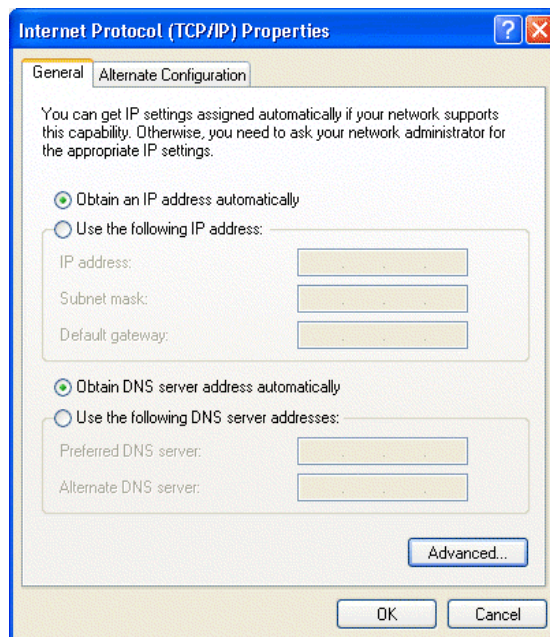
## 5

Verify that the **Obtain an IP address automatically** radio button is selected.

- Verify that **Obtain DNS server address automatically** radio button is selected.
- Click the **OK** button.

This completes the DHCP configuration of TCP/IP in Windows XP.

Repeat these steps for each PC with this version of Windows on your network.



## DHCP Configuration of TCP/IP in Windows 2000

Once again, after you have installed the network card, TCP/IP for Windows 2000 is configured. TCP/IP should be added by default and set to DHCP without your having to configure it.

However, if there are problems, you may need to know how to do it manually. Remember, Cox only sets up TCP/IP dynamically, (i.e., it uses DHCP to obtain TCP/IP settings). Following are the steps to configure TCP/IP with DHCP for Windows 2000.

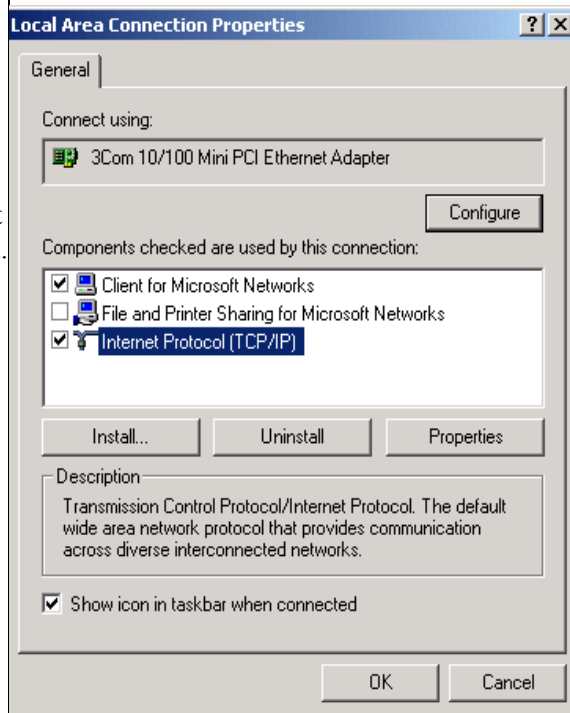
1

- Click on the **My Network Places** icon on the Windows desktop. This will bring up a window called Network and Dial-up Connections.
- Right click on **Local Area Connection** and select **Properties**.

2

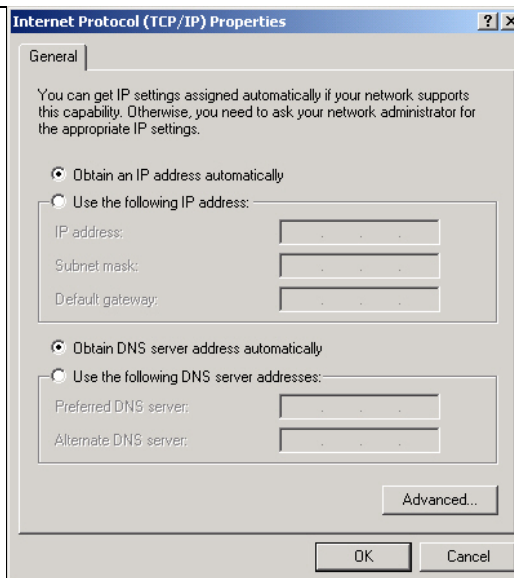
The **Local Area Connection Properties** dialog box appears.

- Verify that you have the correct Ethernet card selected in the **Connect using:** box.
- Verify that at least the following two items are displayed and selected in the box of “Components checked are used by this connection:”
  - Client for Microsoft Networks and
  - Internet Protocol (TCP/IP)
- Click **OK**.



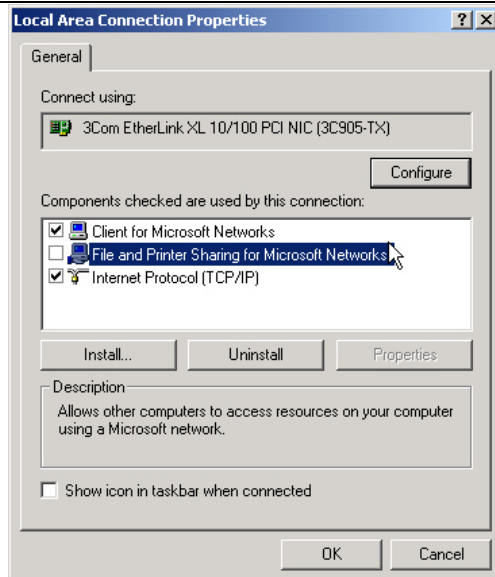
3

- With Internet Protocol (TCP/IP) selected, click on **Properties** to open the Internet Protocol (TCP/IP) Properties dialogue box. Verify that
  - **Obtain an IP address automatically** is selected.
  - **Obtain DNS server address automatically** is selected.
- Click **OK** to return to Local Area Connection Properties.



4

- Click **OK** again to complete the configuration process for Windows 2000.
  - Restart the PC.
- Repeat these steps for each PC with this version of Windows on your network.



## Verifying TCP/IP Properties for Windows XP and 2000

To check your PC's TCP/IP configuration:

1. On the Windows taskbar, click the Start button, and then click Run.

The Run window opens.

2. Type `cmd` and then click OK.

A command window opens

3. Type `ipconfig /all`

Your IP Configuration information will be listed, and should match the values below if you are using the default TCP/IP settings that NETGEAR recommends for connecting through a router or gateway:

- The IP address is between 192.168.0.2 and 192.168.0.254
- The subnet mask is 255.255.255.0
- The default gateway is 192.168.0.1

4. Type `exit`



## Verifying the Readiness of Your Internet Account

---

For broadband access to the Internet, you need to contract with an Internet service provider (ISP) for a single-user Internet access account using a cable modem or DSL modem. This modem must be a separate physical box (not a card) and must provide an Ethernet port intended for connection to a Network Interface Card (NIC) in a computer. Your gateway does not support a USB-connected broadband modem.

For a single-user Internet account, your ISP supplies TCP/IP configuration information for one computer. With a typical account, much of the configuration information is dynamically assigned when your PC is first booted up while connected to the ISP, and you will not need to know that dynamic information.

In order to share the Internet connection among several computers, your gateway takes the place of the single PC, and you need to configure it with the TCP/IP information that the single PC would normally use. When the gateway's Internet port is connected to the broadband modem, the gateway appears to be a single PC to the ISP. The gateway then allows the PCs on the local network to masquerade as the single PC to access the Internet through the broadband modem. The method used by the gateway to accomplish this is called Network Address Translation (NAT) or IP masquerading.

### Are Login Protocols Used?

Some ISPs require a special login protocol, in which you must enter a login name and password in order to access the Internet.

When you configure your gateway, you will need to enter your login name and password in the router's configuration menus. After your network and gateway are configured, the gateway will perform the login task when needed, and you will no longer need to run the login program from your PC. It is not necessary to uninstall the login program.

### What Is Your Configuration Information?

More and more, ISPs are dynamically assigning configuration information. However, if your ISP does not dynamically assign configuration information but instead used fixed configurations, your ISP should have given you the following basic information for your account:

- An IP address and subnet mask
- A gateway IP address, which is the address of the ISP's router
- One or more domain name server (DNS) IP addresses
- Host name and domain suffix

For example, your account's full server names may look like this:

`mail.xxx.yyy.com`

In this example, the domain suffix is `xxx.yyy.com`.

If any of these items are dynamically supplied by the ISP, your gateway automatically acquires them.

If an ISP technician configured your PC during the installation of the broadband modem, or if you configured it using instructions provided by your ISP, you need to copy the configuration information from your PC's Network TCP/IP Properties window or Macintosh TCP/IP Control Panel before reconfiguring your PC for use with the gateway. These procedures are described next.

## Obtaining ISP Configuration Information from Your Computer

As mentioned above, you may need to collect configuration information from your PC so that you can use this information when you configure the CG814WG Gateway. Following this procedure is only necessary when your ISP does not dynamically supply the account information.

To get the information you need to configure the gateway for Internet access:

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Network icon.

The Network window opens, which displays a list of installed components.

3. Select TCP/IP, and then click Properties.

The TCP/IP Properties dialog box opens.

4. Select the IP Address tab.

If an IP address and subnet mask are shown, write down the information. If an address is present, your account uses a fixed (static) IP address. If no address is present, your account uses a dynamically-assigned IP address. Click "Obtain an IP address automatically".

5. Select the Gateway tab.

If an IP address appears under Installed Gateways, write down the address. This is the ISP's gateway address. Select the address and then click Remove to remove the gateway address.

6. Select the DNS Configuration tab.

If any DNS server addresses are shown, write down the addresses. If any information appears in the Host or Domain information box, write it down. Click Disable DNS.

7. Click OK to save your changes and close the TCP/IP Properties dialog box.

You are returned to the Network window.

8. Click OK.

9. Reboot your PC at the prompt. You may also be prompted to insert your Windows CD.

## **Restarting the Network**

---

Once you've set up your computers to work with the gateway, you must reset the network for the devices to be able to communicate correctly. Restart any computer that is connected to the firewall.

After configuring all of your computers for TCP/IP networking and restarting them, and connecting them to the local network of your CG814WG Gateway, you are ready to access and configure the gateway.



## Appendix A

# Troubleshooting

This chapter gives information about troubleshooting your CG814WG Wireless Cable Modem Gateway. For the common problems listed, go to the section indicated.

- Is the gateway on?
- Have I connected the gateway correctly?  
Go to [“Basic Functions” on page A-1.](#)
- I can’t access the gateway’s configuration with my browser.  
Go to [“Troubleshooting the ISP Connection” on page A-3.](#)
- I’ve configured the gateway but I can’t access the Internet.  
Go to [“Troubleshooting the ISP Connection” on page A-3.](#)
- I can’t remember the gateway’s configuration password.
- I want to clear the configuration and start over again.  
Go to [“Erasing the Current/Restoring the Factory Configuration” on page A-5.](#)

## Basic Functions

---

After you turn on power to the gateway, the following sequence of events should occur:

1. When power is first applied, verify that the Power LED is on.
2. Verify that the numbered ethernet LEDs come on momentarily.
3. After approximately 30 seconds, verify that:
  - The Local port Link LEDs are lit for any local ports that are connected.
  - The Test LED is not lit.

- The Internet Link port LED is lit.

If any of these conditions does not occur, refer to the appropriate following section.

## Power LED Not On

If the Power and other LEDs are off when your gateway is turned on:

- Make sure that the power cord is properly connected to your gateway and that the power supply adapter is properly connected to a functioning power outlet.
- Check that you are using the 12VDC power adapter supplied by NETGEAR for this product.

If the error persists, you have a hardware problem and should contact technical support.

## Test LED Stays On

If the Test LED stays on continuously, there is a fault within the gateway.

If you experience problems with the Test LED:

- Cycle the power to see if the gateway recovers and the LED goes off
- If all LEDs including the Test LED are still on one minute after power up, clear the gateway's configuration to factory defaults. This will set the gateway's IP address to 192.168.0.1. This procedure is explained in [“Erasing the Current/Restoring the Factory Configuration”](#) on page A-5.

If the error persists, you might have a hardware problem and should contact technical support.

## Local Link LEDs Not On

If the Local Port Link LEDs do not light when the Ethernet connection is made, check the following:

- Make sure that the Ethernet cable connections are secure at the gateway and at the hub or PC.
- Make sure that power is turned on to the connected hub or PC.
- Be sure you are using the correct cable:
  - When connecting the gateway's Internet port to a cable or DSL modem, use the cable that was supplied with the cable or DSL modem. This cable could be a standard straight-through Ethernet cable or an Ethernet crossover cable.

## Cable Link LED Not On

If the Cable Link LED does not light when connected to your cable television cable, check the following:

- Make sure that the coaxial cable connections are secure at the gateway and at the wall jack.
- Make sure that your cable internet service has been provisioned by your cable service provider. Your provider should verify that the signal quality is good enough for cable modem service.
- Remove any excessive splitters you may have on your cable line. It may be necessary to run a “home run” back to the point where the cable enters your home.

## Troubleshooting the ISP Connection

---

If your gateway is unable to access the Internet and your Cable Link LED is on, you may need to register the Cable MAC Address and/or Device MAC Address of you gateway with your cable service provider. Contact your cable Internet service provider for assistance with this procedure.

Additionally, your PC may not have the gateway configured as its TCP/IP gateway. If your PC obtains its information from the gateway by DHCP, reboot the PC and verify the gateway address as described in [“DHCP Configuration of TCP/IP in Windows 2000 ” on page 2-11.](#)

## Troubleshooting a TCP/IP Network Using a Ping Utility

---

Most TCP/IP terminal devices and routers contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. Troubleshooting a TCP/IP network is made easier by using the ping utility in your PC or workstation.

## Testing the LAN Path to Your Gateway

You can ping the gateway from your PC to verify that the LAN path to your gateway is set up correctly.

To ping the gateway from a PC running Windows 95 or later:

1. From the Windows toolbar, click on the Start button and select Run.
2. In the field provided, type Ping followed by the IP address of the gateway, as in this example:

```
ping 192.168.0.1
```

3. Click on OK.

You should see a message like this one:

```
Pinging <IP address> with 32 bytes of data
```

If the path is working, you see this message:

```
Reply from < IP address >: bytes=32 time=NN ms TTL=xxx
```

If the path is not working, you see this message:

```
Request timed out
```

If the path is not functioning correctly, you could have one of the following problems:

- Wrong physical connections
  - Make sure the LAN port LED is on. If the LED is off, follow the instructions in “[Local Link LEDs Not On](#)” on [page A-2](#).
  - Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and gateway.
- Wrong network configuration
  - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your PC or workstation.
  - Verify that the IP address for your gateway and your workstation are correct and that the addresses are on the same subnet.

## Testing the Path from Your PC to a Remote Device

After verifying that the LAN path works correctly, test the path from your PC to a remote device. From the Windows run menu, type:

```
PING -n 10 <IP address>
```

where *<IP address>* is the IP address of a remote device such as your ISP’s DNS server.

If the path is functioning correctly, replies as in the previous section are displayed. If you do not receive replies:



- Check that your PC has the IP address of your gateway listed as the default gateway. If the IP configuration of your PC is assigned by DHCP, this information will not be visible in your PC's Network Control Panel. Verify that the IP address of the gateway is listed as the default gateway as described in [“DHCP Configuration of TCP/IP in Windows 2000” on page 2-11](#).
- Check to see that the network address of your PC (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- Check that your Cable Link LED is on.
- If your ISP assigned a host name to your PC, enter that host name as the Account Name in the Basic Settings menu.
- Your ISP could be rejecting the Device MAC Address of your gateway because it does not match the MAC Address of the PC you previously used to connect to a cable modem. In this case you will need to clone your PC's MAC Address. Refer to [“Connecting the CG814W Gateway” on page 2-4](#).

## Erasing the Current/Restoring the Factory Configuration

---

The configuration settings of the CG814WG Gateway are stored in a configuration file in the gateway. This file can be reverted to factory default settings. The procedures below explain how to do these tasks.

It is sometimes desirable to restore the gateway to the factory default settings. This can be done by using the Erase function.

1. To erase the configuration, from the Main Menu, under Maintenance select Set Password. Select Yes for Restore Factory Defaults and click Apply.
2. The gateway will then reboot automatically.

After an erase, the gateway's password will be **password**, the LAN IP address will be 192.168.0.1, and the router's DHCP client will be enabled.

**Note:** To restore the factory default configuration settings without knowing the login password or IP address, you must use the Default Reset button on the rear panel of the gateway.

1. Using a paper clip, depress and hold the Default Reset Button. All the numbered Ethernet LEDs will illuminate green.
2. Continue to depress the button for at least 5 seconds.
3. The gateway will reboot and clear its configuration information.



## Appendix B

# Glossary

<b>10BASE-T</b>	IEEE 802.3 specification for 10 Mbps Ethernet over twisted pair wiring.
<b>100BASE-Tx</b>	IEEE 802.3 specification for 100 Mbps Ethernet over twisted pair wiring.
<b>802.11b, 802.11g</b>	IEEE specification for wireless networking at 11 Mbps (802.11b) and 54 Mbps (802.11g) using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.5GHz.
<b>DHCP</b>	<i>See</i> Dynamic Host Configuration Protocol.
<b>DNS</b>	<i>See</i> Domain Name Server.
<b>domain name</b>	A descriptive name for an address or group of addresses on the Internet. Domain names are of the form of a registered entity name plus one of a number of predefined top level suffixes such as .com, .edu, .uk, etc. For example, in the address mail.NETGEAR.com, mail is a server name and NETGEAR.com is the domain.
<b>DOCSIS</b>	Data Over Cable Service Interface Specification. Defines interface requirements for cable modems involved in high-speed data distribution over cable television system networks
<b>Domain Name Server</b>	A Domain Name Server (DNS) resolves descriptive names of network resources (such as www.NETGEAR.com) to numeric IP addresses.
<b>Dynamic Host Configuration Protocol</b>	DHCP. An Ethernet protocol specifying how a centralized DHCP server can assign network configuration information to multiple DHCP clients. The assigned information includes IP addresses, DNS addresses, and gateway (router) addresses.
<b>Gateway</b>	A local device, usually a router, that connects hosts on a local network to other networks.

<b>IETF</b>	Internet Engineering Task Force. An open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. Working groups of the IETF propose standard protocols and procedures for the Internet, which are published as RFCs (Request for Comment) at <a href="http://www.ietf.org">www.ietf.org</a> .
<b>IP</b>	Internet Protocol. The main internetworking protocol used in the Internet. Used in conjunction with the Transfer Control Protocol (TCP) to form TCP/IP.
<b>IP Address</b>	A four-position number uniquely defining each host on the Internet. Ranges of addresses are assigned by Internic, an organization formed for this purpose. Usually written in dotted-decimal notation with periods separating the bytes (for example, 134.177.244.57).
<b>ISP</b>	Internet service provider.
<b>LAN</b>	<i>See</i> local area network.
<b>local area network</b>	LAN. A communications network serving users within a limited area, such as one floor of a building. A LAN typically connects multiple personal computers and shared network devices such as storage and printers. Although many technologies exist to implement a LAN, Ethernet is the most common for connecting personal computers.
<b>MAC address</b>	Media Access Control address. A unique 48-bit hardware address assigned to every Ethernet node. Usually written in the form 01:23:45:67:89:ab.
<b>Mbps</b>	Megabits per second.
<b>MSB</b>	<i>See</i> Most Significant Bit or Most Significant Byte.
<b>MTU</b>	<i>See</i> Maximum Transmit Unit.
<b>Maximum Transmit Unit</b>	The size in bytes of the largest packet that can be sent or received.
<b>NAT</b>	<i>See</i> Network Address Translation.
<b>netmask</b>	A number that explains which part of an IP address comprises the network address and which part is the host address on that network. It can be expressed in dotted-decimal notation or as a number appended to the IP address. For example, a 28-bit mask starting from the MSB can be shown as 255.255.255.192 or as /28 appended to the IP address.
<b>Network Address Translation</b>	A technique by which several hosts share a single IP address for access to the Internet.

<b>packet</b>	A block of information sent over a network. A packet typically contains a source and destination network address, some protocol and length information, a block of data, and a checksum.
<b>PPP</b>	<i>See</i> Point-to-Point Protocol.
<b>Point-to-Point Protocol</b>	PPP. A protocol allowing a computer using TCP/IP to connect directly to the Internet.
<b>RFC</b>	Request For Comment. Refers to documents published by the Internet Engineering Task Force (IETF) proposing standard protocols and procedures for the Internet. RFCs can be found at <a href="http://www.ietf.org">www.ietf.org</a> .
<b>RIP</b>	<i>See</i> Routing Information Protocol.
<b>router</b>	A device that forwards data between networks. An IP router forwards data based on IP source and destination addresses.
<b>Routing Information Protocol</b>	A protocol in which routers periodically exchange information with one another so that they can determine minimum distance paths between sources and destinations.
<b>subnet mask</b>	<i>See</i> netmask.
<b>URL</b>	Universal Resource Locator, the global address of documents and other resources on the World Wide Web.
<b>UTP</b>	Unshielded twisted pair. The cable used by 10BASE-T and 100BASE-Tx Ethernet networks.
<b>WAN</b>	<i>See</i> wide area network.
<b>WEP</b>	Wired Equivalent Privacy. WEP is a data encryption protocol for 802.11b and 802.11g wireless networks. All wireless nodes and access points on the network are configured with a 64-bit or 128-bit Shared Key for data encryption.
<b>wide area network</b>	WAN. A long distance link used to extend or connect remotely located local area networks. The Internet is a large WAN.



## Appendix C

# Configuring Wireless Security in Windows XP

This section describes how to configure basic wireless security on your Wireless Local Area Network (WLAN) when using Windows XP.



**Note:** Indoors, computers can easily connect to 802.11 wireless networks at distances of several hundred feet. Because walls do not always block wireless signals, others outside your immediate area could access your network. It is important to take appropriate steps to secure your network from unauthorized access. The CG814WG provides highly effective security features which are covered in the Comcast user manual. Deploy the security features appropriate to your needs.

## What You Will Need Before You Begin

---

You need to verify your computer meets the minimum system requirements and identify the wireless network configuration settings of the WLAN where you will connect before you can configure your wireless pc card and connect.

## Observe Location and Range Guidelines

Computers can connect over 802.11 wireless networks indoors at a range which vary significantly based on the physical location of the computer with the CG814WG Wireless Cable Modem Gateway. For best results, avoid potential sources of interference, such as:

- Large metal surfaces
- Microwaves
- 2.4 GHz Cordless phones

In general, 802.11 wireless devices can communicate through walls. However, if the walls are constructed with concrete, or have metal, or metal mesh, the 802.11 effective range will decrease if such materials are between the devices.

## Two Basic Operating Modes

---

The CG814WG Gateway, like all 802.11 adapters, can operate in the following two basic modes:

- **Infrastructure Mode:** An 802.11 networking framework in which devices and computers communicate with each other by first going through an access point (AP). For example, this mode is used when computers in a house connect to an Access Point that is attached to a router which lets multiple computers share a single Cable or DSL broadband Internet connection.
- **Ad-Hoc Mode:** An 802.11 networking framework in which devices or computers communicate directly with each other, without the use of an AP. For example, Ad-Hoc Mode is used when two Windows computers are configured with file and print sharing enabled and you want to exchange files directly between them.

Infrastructure configuration procedures for basic network connectivity are covered below. The CG814WG does not operate in Ad-Hoc mode.



## CG814WG Default Wireless Configuration Settings

---

If this is a new wireless network installation, use the factory default settings to set up the network and verify wireless connectivity. If this is an addition to an existing wireless network, you will need to identify the wireless configuration and security parameters already defined.

Your CG814WG Wireless Cable Modem Gateway factory default basic settings are:

- Network Name Service Set Identification (SSID): **NETGEAR**  
**Note:** In order for the CG814WG Gateway to communicate with a wireless access point or wireless adapter, all devices must be configured with the same wireless network name (SSID).
- Network Mode (Infrastructure or Ad-hoc): **Infrastructure**
- Data security WEP encryption: **Disabled**

The section below provides instructions for setting up the CG814WG Wireless Cable Modem Gateway for basic wireless connectivity to an access point. The procedures below provide step-by-step installation instructions for Windows PCs. Use the procedure that corresponds to the version of Windows you are using.

## Basic Installation Instructions

Use the procedure below that corresponds to the version of Windows you are using.

### For Windows XP Users Installing a CG814WG

1

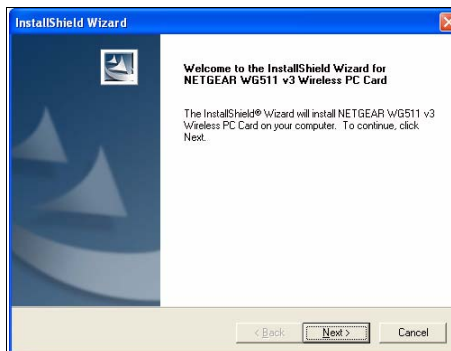
#### Install the CG814WG driver and configuration utility software.

- a. Power on your notebook, let the operating system boot up completely, and log in as needed.
- b. Insert the Resource CD for the CG814WG into your CD-ROM drive. The CD main page shown at the right will load.
- c. Click the “Install Driver & Utility” link.
- d. Follow the Install Shield Wizard steps, and click Finish when done to restart your computer.



CG814WG Resource CD

**Note:** If this page does not automatically appear, browse the root of the CD and double-click on INDEX.HTM to display this page.



Install Shield Wizard

**Note:** If a Windows XP Certification warning appears, click **Continue Anyway** to proceed.

2

**Install the CG814WG Wireless Cable Modem Gateway.**

- a. Locate an available CardBus slot on the side of your notebook. Hold the PC Card with the Netgear logo facing up and insert it into the CardBus slot.

The Found New Hardware Wizard is displayed.

- b. Click **Next** and follow the prompts to proceed.

Click **Continue Anyway** if you are prompted with a Windows XP Logo testing message.

After the installation completes, click **Finish** to close the wizard.

You should see the CG814WG system tray icon on the right in the lower right portion of the Windows task bar.

Windows XP will display a Wireless Network Connection message.



Add New Hardware Wizard



CG814WG System Tray Icon



Windows XP Network Connection Alert

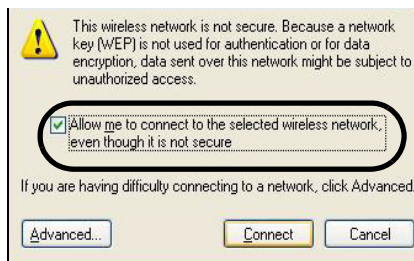
3

**Configure your CG814WG.**

- a. Right click on the network icon in the Windows XP system tray to open the network options menu.
- b. Click on the View Available Wireless Networks menu item.
- c. If there is more than one wireless network in your vicinity, click on the one to which you will connect.
- d. Click on the “Allow me to connect to the selected wireless network even though this is not secure” check box.
- e. Click Connect.



Right click here to display this menu.




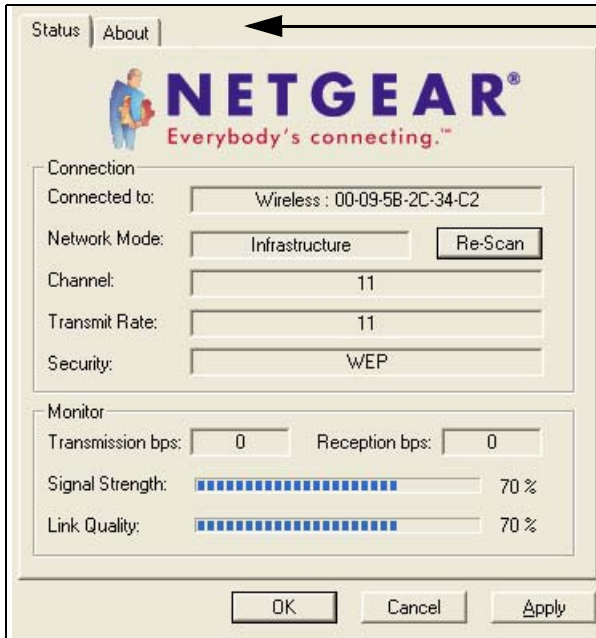
Windows XP Network Connection Alert

**Note:** This procedure assumes your wireless network is not using WEP security. If your wireless network uses WEP, set up your CG814WG accordingly. To view WEP settings help, click the Advanced button and click the “Learn about...” link on the Windows XP Local Area Connection Wireless Networks Properties tab page.

**4**

**Verify wireless connectivity to your network.**

- a. Open the CG814WG utility by clicking on the icon  in the Windows system tray.



**Note:** When the Windows XP wireless configuration utility is enabled (the default), only these two tab pages appear.

To use the full Netgear utility, please see uncheck the “Use Windows to configure your wireless network in the properties of the wireless adapter.

- b. Verify that your Connection and Status Monitor information matches your wireless network.
- c. Check the two CG814WG LEDs:
- Solid green for the LINK LED indicates a good connection. Blinking for the LINK LED indicates attempting to connect. Off for the LINK LED indicates the card is turned off or not fully plugged in.
  - Blinking for the amber transmission LED indicates data transmission.
- d. Verify connectivity to the Internet or network resources.

**Note:** If you are unable to connect, see “[Basic Troubleshooting Tips](#)“ on page C-10.

## Wireless Connection Indicators

---

The NETGEAR wireless adapters provide the indicators which give you feedback on the status of your wireless connection:

- LEDs on the wireless adapter indicate the condition of wireless link.
- The color of the SysTray icon is on the System Tray portion of the taskbar in the Microsoft Windows desktop indicates the status of the connection.

### Interpreting the LED on the CG814WG




These LEDs are described below.

**Table 2-1: LED Descriptions**

LED	Activity	Description
LINK -- Green	On	The card is plugged in to the notebook PC.
	Blinking	Blinking indicates the CG814WG is trying to establish a connection but is unable to do so.
ACTIVITY -- Amber	On/Blinking	If blinking, the CG814WG is has a connection and is transmitting or receiving data.
	Off	There is no wireless network connection.

## Interpreting System Tray Icon Colors

The System Tray (SysTray) resides on one end of the taskbar in the Microsoft Windows desktop.

Color	Condition	Description
<b>Red</b> 	The wireless PC Card has no connection to any other wireless node.	The wireless PC Card is not able to link to any other wireless node or the link is lost. Check your configuration or try moving to a location where the wireless signal quality is better.
<b>Yellow</b> 	The wireless PC Card has a connection with another wireless node.	The wireless link is weak. You may need to move to a better spot, such as closer to the wireless access point. Also, look for possible interference such as a 2.4 GHz cordless phone or large metal surface.
<b>Green</b> 	The wireless PC Card has a connection with another wireless node.	The wireless PC Card has established good communication with an access point and the signal quality is strong.

## Basic Troubleshooting Tips

---

If you have problems connected to your wireless network, try the tips below.

Symptom	Cause	Solution
The PC Card LINK LED is not lit.	The wireless adapter is not inserted into the slot properly or its software is not loaded.	Remove and reinsert the wireless adapter. Check the Windows device manager to see if the PC Card is recognized and enabled. Reload the wireless adapter software, if necessary. Try to install the wireless adapter in a different CardBus slot on your system if one is available.
The LINK LED is blinking repeatedly.	The wireless adapter is attempting to connect to access point but cannot connect.	The access point may not be powered on. Or, the access point and the PC card are not configured with the same wireless parameters. Check the SSID and WEP settings.
I can connect to an access point, but I cannot connect to other computers on the network or the Internet.	This could be a physical layer problem or a network configuration problem.	Check to make sure that the access point is physically connected to the Ethernet network. Make sure that the IP addresses and the Windows networking parameters are all configured correctly. Restart the cable or DSL modem, router, access point, and notebook PC.

Also, for problems with accessing network resources, the Windows software might not be installed and configured properly on your computers. Please refer to Windows documentation for instructions on these options.



## Appendix D

# Networks, Routing, and Firewall Basics

This chapter provides an overview of IP networks, routing, and firewalls.

### Related Publications

---

As you read this document, you may be directed to various RFC documents for further information. An RFC is a Request For Comment (RFC) published by the Internet Engineering Task Force (IETF), an open organization that defines the architecture and operation of the Internet. The RFC documents outline and define the standard protocols and procedures for the Internet. The documents are listed on the World Wide Web at [www.ietf.org](http://www.ietf.org) and are mirrored and indexed at many other sites worldwide.

### Basic Router Concepts

---

Large amounts of bandwidth can be provided easily and relatively inexpensively in a local area network (LAN). However, providing high bandwidth between a local network and the Internet can be very expensive. Because of this expense, Internet access is usually provided by a slower-speed wide-area network (WAN) link such as a cable or DSL modem. In order to make the best use of the slower WAN link, a mechanism must be in place for selecting and transmitting only the data traffic meant for the Internet. The function of selecting and forwarding this data is performed by a router.

## What is a Router?

A router is a device that forwards traffic between networks based on network layer information in the data and on routing tables maintained by the router. In these routing tables, a router builds up a logical picture of the overall network by gathering and exchanging information with other routers in the network. Using this information, the router chooses the best path for forwarding network traffic.

Routers vary in performance and scale, number of routing protocols supported, and types of physical WAN connection they support. The CG814WG Wireless Cable Modem Gateway is a small office router that routes the IP protocol over a single-user broadband connection.

## Routing Information Protocol

One of the protocols used by a router to build and maintain a picture of the network is the Routing Information Protocol (RIP). Using RIP, routers periodically update one another and check for changes to add to the routing table.

The CG814WG Gateway supports both the older RIP-1 and the newer RIP-2 protocols. Among other improvements, RIP-2 supports subnet and multicast protocols. RIP is not required for most home applications.

## IP Addresses and the Internet

Because TCP/IP networks are interconnected across the world, every machine on the Internet must have a unique address to make sure that transmitted data reaches the correct destination. Blocks of addresses are assigned to organizations by the Internet Assigned Numbers Authority (IANA). Individual users and small organizations may obtain their addresses either from the IANA or from an Internet service provider (ISP). You can contact IANA at [www.iana.org](http://www.iana.org).

The Internet Protocol (IP) uses a 32-bit address structure. The address is usually written in dot notation (also called dotted-decimal notation), in which each group of eight bits is written in decimal form, separated by decimal points.

For example, the following binary address:

```
11000011 00100010 00001100 00000111
```

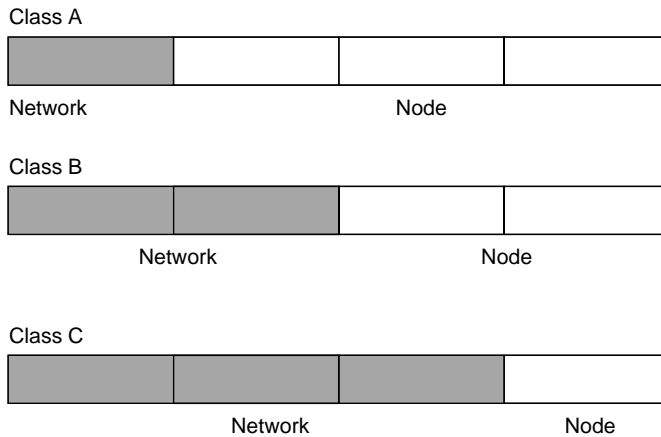
is normally written as:

```
195.34.12.7
```

The latter version is easier to remember and easier to enter into your computer.

In addition, the 32 bits of the address are subdivided into two parts. The first part of the address identifies the network, and the second part identifies the host node or station on the network. The dividing point may vary depending on the address range and the application.

There are five standard classes of IP addresses. These address classes have different ways of determining the network and host sections of the address, allowing for different numbers of hosts on a network. Each address type begins with a unique bit pattern, which is used by the TCP/IP software to identify the address class. After the address class has been determined, the software can correctly identify the host section of the address. The follow figure shows the three main address classes, including network and host sections of the address for each address type.



**Figure D-1: Three Main Address Classes**

The five address classes are:

- **Class A**  
Class A addresses can have up to 16,777,214 hosts on a single network. They use an eight-bit network number and a 24-bit node number. Class A addresses are in this range:

1.x.x.x to 126.x.x.x.

- **Class B**  
Class B addresses can have up to 65,354 hosts on a network. A Class B address uses a 16-bit network number and a 16-bit node number. Class B addresses are in this range:

128.1.x.x to 191.254.x.x.

- Class C  
Class C addresses can have 254 hosts on a network. Class C addresses use 24 bits for the network address and eight bits for the node. They are in this range:  
192.0.1.x to 223.255.254.x.
- Class D  
Class D addresses are used for multicasts (messages sent to many hosts). Class D addresses are in this range:  
224.0.0.0 to 239.255.255.255.
- Class E  
Class E addresses are for experimental use.

This addressing structure allows IP addresses to uniquely identify each physical network and each node on each physical network.

For each unique value of the network portion of the address, the base address of the range (host address of all zeros) is known as the network address and is not usually assigned to a host. Also, the top address of the range (host address of all ones) is not assigned, but is used as the broadcast address for simultaneously sending a packet to all hosts with the same network address.

## Netmask

In each of the address classes previously described, the size of the two parts (network address and host address) is implied by the class. This partitioning scheme can also be expressed by a netmask associated with the IP address. A netmask is a 32-bit quantity that, when logically combined (using an AND operator) with an IP address, yields the network address. For instance, the netmasks for Class A, B, and C addresses are 255.0.0.0, 255.255.0.0, and 255.255.255.0, respectively.

For example, the address 192.168.170.237 is a Class C IP address whose network portion is the upper 24 bits. When combined (using an AND operator) with the Class C netmask, as shown here, only the network portion of the address remains:

```
11000000 10101000 10101010 11101101 (192.168.170.237)
```

combined with:

```
11111111 11111111 11111111 00000000 (255.255.255.0)
```

Equals:

```
11000000 10101000 10101010 00000000 (192.168.170.0)
```

As a shorter alternative to dotted-decimal notation, the netmask may also be expressed in terms of the number of ones from the left. This number is appended to the IP address, following a backward slash (/), as “/n.” In the example, the address could be written as 192.168.170.237/24, indicating that the netmask is 24 ones followed by 8 zeros.

## Subnet Addressing

By looking at the addressing structures, you can see that even with a Class C address, there are a large number of hosts per network. Such a structure is an inefficient use of addresses if each end of a routed link requires a different network number. It is unlikely that the smaller office LANs would have that many devices. You can resolve this problem by using a technique known as subnet addressing.

Subnet addressing allows us to split one IP network address into smaller multiple physical networks known as subnetworks. Some of the node numbers are used as a subnet number instead. A Class B address gives us 16 bits of node numbers translating to 64,000 nodes. Most organizations do not use 64,000 nodes, so there are free bits that can be reassigned. Subnet addressing makes use of those bits that are free, as shown below.



**Figure D-2: Example of Subnetting a Class B Address**

A Class B address can be effectively translated into multiple Class C addresses. For example, the IP address of 172.16.0.0 is assigned, but node addresses are limited to 255 maximum, allowing eight extra bits to use as a subnet address. The IP address of 172.16.97.235 would be interpreted as IP network address 172.16, subnet number 97, and node number 235. In addition to extending the number of addresses available, subnet addressing provides other benefits. Subnet addressing allows a network manager to construct an address scheme for the network by using different subnets for other geographical locations in the network or for other departments in the organization.

Although the preceding example uses the entire third octet for a subnet address, note that you are not restricted to octet boundaries in subnetting. To create more network numbers, you need only shift some bits from the host address to the network address. For instance, to partition a Class C network number (192.68.135.0) into two, you shift one bit from the host address to the network address. The new netmask (or subnet mask) is 255.255.255.128. The first subnet has network number 192.68.135.0 with hosts 192.68.135.1 to 192.68.135.126, and the second subnet has network number 192.68.135.128 with hosts 192.68.135.129 to 192.68.135.254.



**Note:** The number 192.68.135.127 is not assigned because it is the broadcast address of the first subnet. The number 192.68.135.128 is not assigned because it is the network address of the second subnet.

The following table lists the additional subnet mask bits in dotted-decimal notation. To use the table, write down the original class netmask and replace the 0 value octets with the dotted-decimal value of the additional subnet bits. For example, to partition your Class C network with subnet mask 255.255.255.0 into 16 subnets (4 bits), the new subnet mask becomes 255.255.255.240.

**Table D-1. Netmask Notation Translation Table for One Octet**

Number of Bits	Dotted-Decimal Value
1	128
2	192
3	224
4	240
5	248
6	252
7	254
8	255

The following table displays several common netmask values in both the dotted-decimal and the mask length formats.

**Table D-2. Netmask Formats**

Dotted-Decimal	Masklength
255.0.0.0	/8
255.255.0.0	/16

**Table D-2. Netmask Formats**

---

255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30
255.255.255.254	/31
255.255.255.255	/32

---

NETGEAR strongly recommends that you configure all hosts on a LAN segment to use the same netmask for the following reasons:

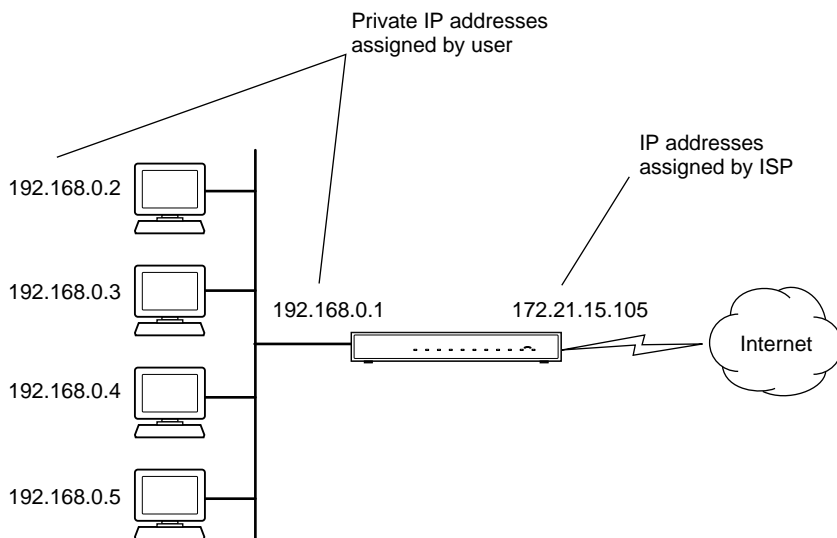
- So that hosts recognize local IP broadcast packets  
When a device broadcasts to its segment neighbors, it uses a destination address of the local network address with all ones for the host address. In order for this scheme to work, all devices on the segment must agree on which bits comprise the host address.
- So that a local router or bridge recognizes which addresses are local and which are remote

## Single IP Address Operation Using NAT

In the past, if multiple PCs on a LAN needed to access the Internet simultaneously, you had to obtain a range of IP addresses from the ISP. This type of Internet account is more costly than a single-address account typically used by a single user with a modem, rather than a router. The CG814WG Gateway employs an address-sharing method called Network Address Translation (NAT). This method allows several networked PCs to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your ISP.

The router accomplishes this address sharing by translating the internal LAN IP addresses to a single address that is globally unique on the Internet. The internal LAN IP addresses can be either private addresses or registered addresses. For more information about IP address translation, refer to RFC 1631, *The IP Network Address Translator (NAT)*.

The following figure illustrates a single IP address operation.



**Figure D-3: Single IP Address Operation Using NAT**

This scheme offers the additional benefit of firewall-like protection because the internal LAN addresses are not available to the Internet through the translated connection. All incoming inquiries are filtered out by the router. This filtering can prevent intruders from probing your system. However, using port forwarding, you can allow one PC (for example, a Web server) on your local network to be accessible to outside users.

## MAC Addresses and Address Resolution Protocol

An IP address alone cannot be used to deliver data from one LAN device to another. To send data between LAN devices, you must convert the IP address of the destination device to its media access control (MAC) address. Each device on an Ethernet network has a unique MAC address, which is a 48-bit number assigned to each device by the manufacturer. The technique that associates the IP address with a MAC address is known as address resolution. Internet Protocol uses the Address Resolution Protocol (ARP) to resolve MAC addresses.



If a device sends data to another station on the network and the destination MAC address is not yet recorded, ARP is used. An ARP request is broadcast onto the network. All stations on the network receive and read the request. The destination IP address for the chosen station is included as part of the message so that only the station with this IP address responds to the ARP request. All other stations discard the request.

## Related Documents

The station with the correct IP address responds with its own MAC address directly to the sending device. The receiving station provides the transmitting station with the required destination MAC address. The IP address data and MAC address data for each station are held in an ARP table. The next time data is sent, the address can be obtained from the address information in the table.

For more information about address assignment, refer to the IETF documents RFC 1597, *Address Allocation for Private Internets*, and RFC 1466, *Guidelines for Management of IP Address Space*.

For more information about IP address translation, refer to RFC 1631, *The IP Network Address Translator (NAT)*.

## Domain Name Server

Many of the resources on the Internet can be addressed by simple descriptive names such as *www.NETGEAR.com*. This addressing is very helpful at the application level, but the descriptive name must be translated to an IP address in order for a user to actually contact the resource. Just as a telephone directory maps names to phone numbers, or as an ARP table maps IP addresses to MAC addresses, a domain name system (DNS) server maps descriptive names of network resources to IP addresses.

When a PC accesses a resource by its descriptive name, it first contacts a DNS server to obtain the IP address of the resource. The PC sends the desired message using the IP address. Many large organizations, such as ISPs, maintain their own DNS servers and allow their customers to use the servers to look up addresses.

## IP Configuration by DHCP

When an IP-based local area network is installed, each PC must be configured with an IP address. If the PCs need to access the Internet, they should also be configured with a gateway address and one or more DNS server addresses. As an alternative to manual configuration, there is a method by which each PC on the network can automatically obtain this configuration information. A device on the network may act as a Dynamic Host Configuration Protocol (DHCP) server. The DHCP server stores a list or pool of IP addresses, along with other information (such as gateway and DNS addresses) that it may assign to the other devices on the network. The CG814WG Gateway has the capacity to act as a DHCP server.

The CG814WG Gateway also functions as a DHCP client when connecting to the ISP. The gateway can automatically obtain an IP address, subnet mask, DNS server addresses, and a gateway address if the ISP provides this information by DHCP.

## Internet Security and Firewalls

---

When your LAN connects to the Internet through a router, an opportunity is created for outsiders to access or disrupt your network. A NAT router provides some protection because by the very nature of the Network Address Translation (NAT) process, the network behind the NAT router is shielded from access by outsiders on the Internet. However, there are methods by which a determined hacker can possibly obtain information about your network or at the least can disrupt your Internet access. A greater degree of protection is provided by a firewall router.

### What is a Firewall?

A firewall is a device that protects one network from another, while allowing communication between the two. A firewall incorporates the functions of the NAT router, while adding features for dealing with a hacker intrusion or attack. Several known types of intrusion or attack can be recognized when they occur. When an incident is detected, the firewall can log details of the attempt, and can optionally send email to an administrator notifying them of the incident. Using information from the log, the administrator can take action with the ISP of the hacker. In some types of intrusions, the firewall can fend off the hacker by discarding all further packets from the hacker's IP address for a period of time.

## Stateful Packet Inspection

Unlike simple Internet sharing routers, a firewall uses a process called stateful packet inspection to ensure secure firewall filtering to protect your network from attacks and intrusions. Since user-level applications such as FTP and Web browsers can create complex patterns of network traffic, it is necessary for the firewall to analyze groups of network connection “states.” Using Stateful Packet Inspection, an incoming packet is intercepted at the network layer and then analyzed for state-related information associated with all network connections. A central cache within the firewall keeps track of the state information associated with all network connections. All traffic passing through the firewall is analyzed against the state of these connections in order to determine whether or not it will be allowed to pass through or rejected.

## Ethernet Cabling

---

Although Ethernet networks originally used thick or thin coaxial cable, most installations currently use unshielded twisted pair (UTP) cabling. The UTP cable contains eight conductors, arranged in four twisted pairs, and terminated with an RJ45 type connector. A normal "straight-through" UTP Ethernet cable follows the EIA568B standard wiring as described in [Table D-1](#).

**Table D-1. UTP Ethernet cable wiring, straight-through**

Pin	Wire color	Signal
1	Orange/White	Transmit (Tx) +
2	Orange	Transmit (Tx) -
3	Green/White	Receive (Rx) +
4	Blue	
5	Blue/White	
6	Green	Receive (Rx) -
7	Brown/White	
8	Brown	

## Uplink Switches and Crossover Cables

In the wiring table, the concept of transmit and receive are from the perspective of the PC. For example, the PC transmits on pins 1 and 2. At the hub, the perspective is reversed, and the hub receives on pins 1 and 2. When connecting a PC to a PC, or a hub port to another hub port, the

transmit pair must be exchanged with the receive pair. This exchange is done by one of two mechanisms. Most hubs provide an Uplink switch which will exchange the pairs on one port, allowing that port to be connected to another hub using a normal Ethernet cable. The second method is to use a crossover cable, which is a special cable in which the transmit and receive pairs are exchanged at one of the two cable connectors. Crossover cables are often unmarked as such, and must be identified by comparing the two connectors. Since the cable connectors are clear plastic, it is easy to place them side by side and view the order of the wire colors on each. On a straight-through cable, the color order will be the same on both connectors. On a crossover cable, the orange and blue pairs will be exchanged from one connector to the other.

## **Cable Quality**

A twisted pair Ethernet network operating at 10 Mbits/second (10BASE-T) will often tolerate low quality cables, but at 100 Mbits/second (10BASE-Tx) the cable must be rated as Category 5, or "Cat 5", by the Electronic Industry Association (EIA). This rating will be printed on the cable jacket. A Category 5 cable will meet specified requirements regarding loss and crosstalk. In addition, there are restrictions on maximum cable length for both 10 and 100 Mbits/second networks.